ZASSENHAUS CONJECTURE ON TORSION UNITS HOLDS FOR SL(2, p) AND SL(2, p^2)

ÁNGEL DEL RÍO AND MARIANO SERRANO

Abstract. H.J. Zassenhaus conjectured that any unit of finite order and augmentation 1 in the integral group ring $\mathbb{Z}G$ of a finite group $G$ is conjugate in the rational group algebra $\mathbb{Q}G$ to an element of $G$. We prove the Zassenhaus Conjecture for the groups $\text{SL}(2, p)$ and $\text{SL}(2, p^2)$ with $p$ a prime number. This is the first infinite family of non-solvable groups for which the Zassenhaus Conjecture has been proved. We also prove that if $G = \text{SL}(2, p^f)$, with $f$ arbitrary and $u$ is a torsion unit of $\mathbb{Z}G$ with augmentation 1 and order coprime with $p$ then $u$ is conjugate in $\mathbb{Q}G$ to an element of $G$. By known results, this reduces the proof of the Zassenhaus Conjecture for this groups to prove that every unit of $\mathbb{Z}G$ of order multiple of $p$ and augmentation 1 has actually order $p$.

1. Introduction

For a finite group $G$, let $V(\mathbb{Z}G)$ denote the group of units of augmentation 1 in $\mathbb{Z}G$. We say that two elements of $\mathbb{Z}G$ are rationally conjugate if they are conjugate in the units of $\mathbb{Q}G$. The following conjecture stated by H.J. Zassenhaus [Zas74] (see also [Seh93, Section 37]) has centered the research on torsion units of integral group rings during the last decades:

Zassenhaus Conjecture: If $G$ is a finite group then every torsion element of $V(\mathbb{Z}G)$ is rationally conjugate to an element of $G$.

The relevance of the Zassenhaus Conjecture is that it describes the torsion units of the integral group ring of $\mathbb{Z}G$ provided it holds for $G$. Recently, Eisele and Margolis announced a metabelian counterexample to the Zassenhaus Conjecture [EM18]. Nevertheless, the Zassenhaus Conjecture holds for large classes of solvable groups, e.g. for nilpotent groups [Wei91], groups possessing a normal Sylow subgroup with abelian complement [Her06] or cyclic-by-abelian groups [CMR13]. In contrast with these results, the list of non-solvable groups for which the Zassenhaus Conjecture has been proved is very limited [LP89, DJPM97, Her07, Her08, BH08, BKL08, BM17c, RS17]. For example, the Zassenhaus Conjecture has only been proved for sixty-two simple groups, all of them of the form $\text{PSL}(2, q)$ (see the proof of Theorem C in [BM18] and [MRS18]).

The goal of this paper is proving the following theorem:

Theorem 1.1. Let $G = \text{SL}(2, q)$ with $q$ an odd prime power and let $u$ be a torsion element of $V(\mathbb{Z}G)$ of order coprime with $q$. Then $u$ is rationally conjugate to an element of $G$.

As a consequence of Theorem 1.1 and known results we will obtain the following theorem which provides the first positive result on the Zassenhaus Conjecture for an infinite series of non-solvable groups.

Theorem 1.2. The Zassenhaus Conjecture holds for $\text{SL}(2, p^f)$ with $p$ a prime number and $f \leq 2$.

In Section 2 we prove a number theoretical result relevant for our arguments. Known results on $V(\mathbb{Z}G)$ and properties of $V(\mathbb{Z}\text{SL}(2, q))$ are collected in Section 3. A particular case of Theorem 1.1 is proved in Section 4. Finally in Section 5 we prove Theorem 1.1.
2. Number theoretical preliminaries

We use the standard notation for the Euler totient function $\varphi$ and the Möbius function $\mu$. Moreover, $\mathbb{Z}_{\geq 0}$ denotes the set of non-negative integers. Let $n$ be a positive integer. Then $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, $\zeta_n$ denotes a complex primitive $n$-th root of unity, $\Phi_n(X)$ denotes the $n$-th cyclotomic polynomial, i.e. the minimal polynomial of $\zeta_n$ over $\mathbb{Q}$, and for a prime integer $p$ let $v_p(n)$ denote the valuation of $n$ at $p$, i.e. the maximum non-negative integer $m$ with $p^m \mid n$. If $F/K$ is a finite field extension then $\text{Tr}_{F/K} : F \to K$ denotes the standard trace map. We will frequently use the following formula for $d$ a divisor of $n$ [Mar16, Lemma 2.1]:

\begin{equation}
\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)} = \mu(d) \frac{\varphi(n)}{\varphi(d)}.
\end{equation}

We reserve the letter $p$ to denote a positive prime integer and for every positive integer $n$ we set

$$n' = \prod_{p \mid n} p \quad \text{and} \quad n_p = p^{v_p(n)}.$$ 

If moreover $x \in \mathbb{Z}$ then we set

$$(x : n) = \text{representative of the class of } x \text{ modulo } n \text{ in the interval } \left(-\frac{n}{2}, \frac{n}{2}\right);$$

$$|x : n| = \text{the absolute value of } (x : n);$$

$$\gamma_n(x) = \prod_{\substack{p \mid n \implies \frac{n_p}{n_p} \neq \frac{1}{2} \mod n_p}} p \quad \text{and} \quad \bar{\gamma}_n(x) = \prod_{\substack{p \mid n \implies \frac{n_p}{n_p} \leq \frac{1}{2} \mod n_p}} p = \begin{cases} 2\gamma_n(x), & \text{if } |x : n_2| = \frac{n_2}{2}; \\ \gamma_n(x), & \text{otherwise}. \end{cases}$$

The next lemma collects two facts which follow easily from the definitions.

**Lemma 2.1.** Let $p$ be a prime dividing $n$ and let $x, y \in \mathbb{Z}$. Then the following conditions hold:

1. If $p \mid \bar{\gamma}_n(x)$ then $(x : \frac{n_p}{p}) \equiv x \mod n_p$.
2. Let $d \mid n'$ such that $x \equiv y \mod \frac{n}{d}$. If $d$ divides both $\bar{\gamma}_n(x)$ and $\bar{\gamma}_n(y)$ then $x \equiv y \mod n$.

For integers $x$ and $y$ we define the following equivalence relation on $\mathbb{Z}$:

$$x \sim_n y \iff x \equiv \pm y \mod n.$$ 

We denote by $\Gamma_n$ the set of these equivalence classes.

If $x, y$ and $n$ are integers with $n > 0$ then let

$$\delta^{(n)}_{x,y} = \begin{cases} 1, & \text{if } x \sim_n y; \\ 0, & \text{otherwise}; \end{cases} \quad \text{and} \quad \kappa^{(n)}_{x} = \begin{cases} 2, & \text{if } x \equiv 0 \mod n \text{ or } x \equiv \frac{n}{2} \mod n; \\ 1, & \text{otherwise}. \end{cases}$$

For an integer $x$ (or $x \in \Gamma_n$) we set

$$\alpha^{(n)}_x = \zeta_n^x + \zeta_n^{-x}.$$ 

Observe that $\mathbb{Q}(\alpha^{(n)}_1)$ is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\alpha^{(n)}_1]$ is the ring of integers of $\mathbb{Q}(\alpha^{(n)}_1)$. If $n \neq n_2$ then let $p_0$ denote the smallest odd prime dividing $n$. Then let

$$\mathbb{B}_n = \left\{ x \in \mathbb{Z}_n : \text{for every } p \mid n, \text{ either } |x : n_p| > \frac{n_p}{2} \text{ or } p = 2, n \neq n_2, |x : n_2| = \frac{n_2}{4}, n_{p_0} \mid x \text{ and } (x : n_2) \cdot (x : n_{p_0}) > 0 \right\}$$

and

$$\mathbb{B}_n = \begin{cases} \{ \alpha^{(n)}_b : b \in \mathbb{B}_n \}, & \text{if } n \neq n_2; \\ \{1\} \cup \{ \alpha^{(n)}_b : b \in \mathbb{B}_n \}, & \text{otherwise.} \end{cases}$$
For \( b \in \mathbb{B}_n \) and \( x \in \mathbb{Z} \) let
\[
\beta_{b,x}^{(n)} = \begin{cases} 
-1, & \text{if } n \neq n_2, |x : n_2| = \frac{n_2}{4} \text{ and } (x : n_2) \cdot (b : n_{p_0}) < 0; \\
1, & \text{otherwise}.
\end{cases}
\]

The following proposition extends Proposition 3.5 of [MRS18]. The first statement implies that \( \mathcal{B}_n \) is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\alpha_1^{(n)}) \). For \( x \in \mathbb{Q}(\alpha_1^{(n)}) \) and \( b \in \mathbb{B}_n \) we use \( C_b(x) \) to denote the coefficient of \( \alpha_b^{(n)} \) in the expression of \( x \) in the basis \( \mathcal{B}_n \).

**Proposition 2.2.** Let \( n \) be a positive integer. Then

1. \( \mathcal{B}_n \) is a \( \mathbb{Z} \)-basis of \( \mathbb{Z}[\alpha_1^{(n)}] \).
2. If \( b \in \mathbb{B}_n \) and \( i \in \mathbb{Z} \) then \( C_b(\alpha_i^{(n)}) = \kappa_i^{(n)} \cdot \mu(\gamma(i)) \cdot \beta_{b,i}^{(n)} \cdot \zeta_{b,i}^{(n/\gamma(i))} \).

**Proof.** We only prove the proposition in the case \( n \neq n_2 \), as the proof in the case \( n = n_2 \) is similar (actually simpler). It is easy to see that \( |\mathcal{B}_n| \leq \frac{\varphi(n)}{2} = [\mathbb{Q}(\alpha_1^{(n)}) : \mathbb{Q}] \). Thus it is enough to prove the following equality
\[
\zeta_n^i = \mu(\gamma(i)) \sum_{\substack{b \equiv i \mod n/\gamma(i) \\ b \in \mathbb{B}_n}} \beta_{b,i}^{(n)} \zeta_n^b
\]
which easily implies the desired expression of \( \alpha_i^{(n)} \).

Indeed, for every \( p \mid n \) let \( \zeta_{np} \) denote the \( p \)-th part of \( \zeta_n \), i.e. \( \zeta_{np} \) is a primitive \( n_p \)-th root of unity and \( \zeta_n = \prod_{p \mid n} \zeta_{np} \). Let \( J \) be the set of tuples \( (j_p)_p \) satisfying the following conditions:

- If \( p \mid \gamma(i) \) then \( j_p \in \{1, \ldots, p - 1\} \).
- If \( p = 2 \) and \( |i : n_2| = \frac{n_2}{4} \) then \( j_2 = \begin{cases} 
1, & \text{if } (i : n_2) \cdot (i + j_p \frac{n_{p_0}}{p_0} : n_{p_0}) < 0; \\
0, & \text{otherwise}.
\end{cases} \)

For every \( j \in J \) let \( b_j \in \mathbb{Z}_n \) given by
\[
b_j \equiv \begin{cases} 
i + j_p \frac{n_p}{p} \mod n_p, & \text{if } p \mid \gamma(i); \\
i \mod n_p, & \text{otherwise}.
\end{cases}
\]

Then \( \{b_j : j \in J\} \) is the set of elements in \( \mathbb{B}_n \) satisfying \( i \equiv b \mod n/\gamma(i) \). From
\[
0 = \zeta_n^i \left( 1 + \zeta_{np}^\frac{n_p}{p} + \zeta_{np}^{2n_p/p} + \cdots + \zeta_{np}^{(p-1)n_p/p} \right)
\]
we obtain \( \zeta_{np}^i = -\sum_{j_p=1}^{p-1} \zeta_{np}^{i+j_p \frac{n_p}{p}} \). Therefore, if \( |i : n_2| \neq \frac{n_2}{4} \) then \( \gamma(i) = \bar{\gamma}(i) \), \( \beta_{b,i}^{(n)} = 1 \) for every \( b \in \mathbb{B}_n \) and
\[
\zeta_n^i = \prod_{p \mid n} \zeta_{np}^i \cdot \prod_{p \mid \gamma(i)} \left( -\sum_{j_p=1}^{p-1} \zeta_{np}^{i+j_p \frac{n_p}{p}} \right) = \mu(\gamma(i)) \sum_{j \in J} \beta_{b,j}^{(n)} \zeta_n^j = \mu(\gamma(i)) \sum_{b \equiv i \mod n/\gamma(i)} \beta_{b,i}^{(n)} \zeta_n^b.
\]
This gives the desired equality in this case.

Suppose that \( |i : n_2| = \frac{n_2}{4} \). Then \( \zeta_{n_2}^i = \beta_{b,j}^{(n)} \zeta_{n_2}^j \) for every \( j \in J \). Then a small modification of the argument in the previous paragraph gives
\[
\zeta_n^i = \zeta_{n_2}^i \prod_{p \mid n} \zeta_{np}^i \cdot \prod_{p \mid \gamma(i)} \left( -\sum_{j_p=1}^{p-1} \zeta_{np}^{i+j_p \frac{n_p}{p}} \right) = \mu(\gamma(i)) \sum_{j \in J} \beta_{b,j}^{(n)} \zeta_n^j = \mu(\gamma(i)) \sum_{b \equiv i \mod n/\gamma(i)} \beta_{b,i}^{(n)} \zeta_n^b.
\]
3. Group theoretical preliminaries

Let $G$ be a finite group. We denote by $Z(G)$ the center of $G$. If $g \in G$ then $|g|$ denotes the order of $g$, $\langle g \rangle$ denotes the cyclic group generated by $g$, and $g^G$ denotes the conjugacy class of $g$ in $G$. If $R$ is a ring then $RG$ denotes the group ring of $G$ with coefficients in $R$. If $\alpha = \sum_{g \in G} \alpha_g g$ is an element of a group ring $RG$, with each $\alpha_g \in R$, then the partial augmentation of $\alpha$ at $g$ is defined as

$$\varepsilon_g(\alpha) = \sum_{h \in g^G} \alpha_h.$$ 

We collect here some known results on partial augmentations of an element $u$ of order $n$ in $V(\mathbb{Z}G)$.

(A) [JR16, Proposition 1.5.1] (Berman-Higman Theorem). If $g \in Z(G)$ and $u \neq g$ then $\varepsilon_g(u) = 0$.

(B) [Her07, Theorem 2.3] If $g \in G$ and $\varepsilon_g(u) \neq 0$ then $|g|$ divides $n$.

(C) [MRSW87, Theorem 2.5] $u$ is rationally conjugate to an element of $G$ if and only if $\varepsilon_g(u^d) \geq 0$ for all $g \in G$ and all divisors $d$ of $n$.

(D) [LP89, Her07] Let $F$ be a field of characteristic $t \geq 0$ with $t \nmid n$. Let $\rho$ be an $F$-representation of $G$. If $t \neq 0$ then let $\xi_n$ be a primitive $n$-th root of unity in $F$, so that if $t = 0$ then $\xi_n = \zeta_n$. Let $T$ be a set of representatives of the conjugacy classes of $t$-regular elements of $G$ (all the conjugacy classes if $t = 0$). Let $\chi$ denote the character afforded by $\rho$ if $t = 0$, and the $t$-Brauer character of $G$ afforded by $\rho$ if $t > 0$ (using a group isomorphism associating $\xi_n$ to $\zeta_n$). Then for every integer $\ell$, the multiplicity of $\xi_n^\ell$ as eigenvalue of $\rho(u)$ is

$$\frac{1}{n} \sum_{x \in T} \sum_{d \mid n} \varepsilon_x(u^d) Tr_{\mathbb{Q}(\xi_n^d)/\mathbb{Q}}(\chi(x) \zeta_n^{-\ell d}).$$

In the remainder of the paper we fix an odd prime power $q$ and let $G = \text{SL}(2, q)$, $\overline{G} = \text{PSL}(2, q)$ and let $\pi : G \to \overline{G}$ denote the natural projection, which we extend by linearity to a ring homomorphism $\pi : \mathbb{Z}G \to \mathbb{Z}\overline{G}$.

We collect some group theoretical properties of $G$ and $\overline{G}$ (see e.g. [Dor71, Theorem 38.1]).

(E) $G$ has a unique element $J$ of order 2 and $q + 4$ conjugacy classes. More precisely, if $p$ is the prime dividing $q$ then 2 of the classes are formed by elements of order $p$, another 2 are formed by elements of order $2p$ and $q$ classes are formed by elements of order dividing $q + 1$ or $q - 1$. Furthermore, if $g$ and $h$ are $p$-regular elements of $G$ and $|h|$ divides $|g|$ then $h$ is conjugate in $G$ to an element of $\langle g \rangle$ and two elements of $\langle g \rangle$ are conjugate in $G$ if and only if they are equal or mutually inverse.

(F) Let $C$ be a conjugacy class of $\overline{G}$ formed by elements of order $n$. If $n = 2$ then $\pi^{-1}(C)$ is the only conjugacy class of $G$ formed by elements of order 4. Otherwise, $\pi^{-1}(C)$ is the union of two conjugacy classes $C_1$ and $C_2$ of $G$ with $C_2 = JC_1$. Furthermore, if $n$ is multiple of 4 then the elements of $C_1$ and $C_2$ have order $2n$ while if $n$ is not multiple of 4 then one of the classes $C_1$ or $C_2$ is formed by elements of order $n$.

The following proposition collects some consequences of these facts.

**Proposition 3.1.** Let $G = \text{SL}(2, q)$ and let $u$ be a torsion element of $V(\mathbb{Z}G)$. Set $\overline{G} = \text{PSL}(2, q)$ and $n = |u|$. Then the following statements holds:

1. $J$ is the unique element of order 2 in $V(\mathbb{Z}G)$.
2. $|\pi(u)| = \frac{n}{\gcd(2, n)}$.
3. If $4 \nmid n$ and $\pi(u)$ is rationally conjugate to an element of $\overline{G}$ then $u$ is rationally conjugate to an element of $G$.
4. If $\gcd(n, q) = 1$ and either $n = 4$ or $4 \nmid n$ then $u$ is rationally conjugate to an element of $G$.
5. If $\gcd(n, q) = 1$ then $G$ has an element of order $n$.
6. Suppose that $q = p^f$ with $p$ prime, $f \leq 2$ and $p \mid n$. Then $u$ is rationally conjugate to an element of $G$. 


(7) If \( \rho \) is a representation of \( G \) and \( \zeta \) is a root of unity of order dividing \( n \) then \( \zeta \) and \( \zeta^{-1} \) have the same multiplicity as eigenvalues of \( \rho(u) \).

**Proof.** (1) is a direct consequence of (A) and (E).

(2) By the main result of [Mar17], if \( \pi(u) = 1 \) then \( u^2 = 1 \) and hence either \( u = 1 \) or \( u = J \), by (1). Then (2) follows.

(3) Suppose that \( n \) is not multiple of 4. If \( n \) is even then the order of \( Ju \) is odd, by (1). Thus, we may assume without loss of generality that the order of \( u \) is odd. If \( \varepsilon_g(u) \neq 0 \) then \(|g| \) is odd, by (B), and hence \( \varepsilon_g(u) = \varepsilon_{\pi(g)}(\pi(u)) \geq 0 \), by (F). Thus \( u \) is rationally conjugate to an element of \( G \).

(4) Let \( q = p^k \) where \( p \) is an odd prime number and \( p \not| n \). By (E), \( G \) has a unique conjugacy class \( C \) formed by elements of order 4 and a unique element of order 2. Thus, by (A) and (B), if \( n = 4 \) then \( \varepsilon_g(u) = 0 \) for every \( g \not\in C \), and hence \( u \) is rationally conjugate to an element of \( G \), by (C).

If \( 4 \not| n \) then \(|\pi(u)| \) is coprime with \( 2q \), by (2), and hence \( \pi(u) \) is rationally conjugate to an element of \( \overline{G} \), by [MRS18, Theorem 1.1]. Then \( u \) is rationally conjugate to an element of \( G \) by (3). (5) is a consequence of (2) and [Her07, Proposition 6.7].

(6) In this case \(|\pi(u)| = p \) by (2) and [BM17b, Theorem A]. Then \( n \) is either \( p \) or \( 2p \), by (2), and \( \pi(u) \) is rationally conjugate to an element of \( \overline{G} \), by [Her07, Proposition 6.1]. Thus \( u \) is rationally conjugate to an element of \( G \), by (3).

(7) is a consequence of (E) and the formula in (D). \( \square \)

Observe that for \( q \) odd, Theorem 1.2 follows at once from Theorem 1.1 and statement (6) of Proposition 3.1. On the other hand \( \text{SL}(2,2) \cong S_3 \) and \( \text{SL}(2,4) \cong A_5 \) for which the Zassenhaus Conjecture is well known. So in the remainder of the paper we concentrate on proving Theorem 1.1. For that from now on \( t \) denotes the prime dividing \( q \) (we want to use freely the letter \( p \) to denote an arbitrary prime) and we introduce some \( t \)-Brauer characters of \( G \).

Let \( g \) be an element of \( G \) of order \( n \) with \( t \not| n \) and let \( \xi_n \) denote a primitive \( n \)-th root of unity in a field \( F \) of characteristic \( t \). Adapting the proof of [Mar16, Lemma 1.2] we deduce that for every positive integer \( m \) there is an \( F \)-representation \( \Theta_m \) of \( G \) of degree \( 1 + m \) such that

\[
\Theta_m(g) = \begin{cases} 
\text{diag} \left( 1, \xi_n^2, \xi_n^{-2}, \ldots, \xi_n^m, \xi_n^{-m} \right), & \text{if } 2 \mid m; \\
\text{diag} \left( \xi_n, \xi_n^{-1}, \xi_n^3, \xi_n^{-3}, \ldots, \xi_n^m, \xi_n^{-m} \right), & \text{if } 2 \nmid m.
\end{cases}
\]

In particular, the restriction to \( \langle g \rangle \) of the \( t \)-Brauer character associated to \( \Theta_m \) is given by

\[
\chi_m(g^i) = \sum_{j=-m}^{m} \xi_n^{ij}.
\]

4. **Prime power order**

In this section we prove the following particular case of Theorem 1.1.

**Proposition 4.1.** Let \( G = \text{SL}(2,q) \) with \( q \) an odd prime power and let \( u \) be a torsion element of \( V(\mathbb{Z}G) \). If the order of \( u \) is a prime power and it is coprime with \( q \) then \( u \) is rationally conjugate to an element of \( G \).

**Proof.** By Proposition 3.1.(4) we may assume that \(|u| = 2^r \) with \( r \geq 3 \). We argue by induction on \( r \). So we assume that units of order \( 2^k \) with \( 1 \leq k \leq r - 1 \) are rationally conjugate to an element of \( G \). By Proposition 3.1.(5) and (E), \( G \) has an element \( g_0 \) of order \( 2^r \) such that \( \{g_0^k : k = 0, 1, 2, \ldots, 2^{r-1}\} \) is a set of representatives of the conjugacy classes of \( G \) with order a divisor of \( 2^r \). By (B), the only possible non-zero partial augmentations of
\begin{align*}
\text{if } 0 \leq h \leq r - 2 \text{ and } 2^{r-1} \nmid \ell \text{ then } B(\chi_{2^h}, \ell) &= \begin{cases} 
2^{r-1}, & \text{if } h \geq 1; \\
0, & \text{if } h = 0;
\end{cases}
\end{align*}

and

\begin{align*}
\text{if } 0 \leq h \leq r - 3, 2^h \nmid \ell \text{ and } 2^{r-1} \nmid \ell \text{ then } B(\chi_{2^h}, \ell) &= \begin{cases} 
2^{r-1}, & \text{if } \ell \equiv \pm 2^h \text{ mod } 2^{r-1}; \\
0, & \text{otherwise}.
\end{cases}
\end{align*}

In both cases we argue by induction on \( h \) with the cases \( h = 0 \) and \( h = 1 \) being straightforward. Suppose that \( 1 < h \leq r - 2, 2^{r-1} \nmid \ell \) and \( B(\chi_{2^h}, \ell) = 2^{r-1} \). If \( j \) is even, then straightforward calculations show that

\begin{align*}
\sum_{k=0}^{r-1} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} (\zeta_{2^k}^{2h-1+j} + \zeta_{2^k}^{-2h-1-j}) = 0.
\end{align*}

This implies that \( B(\chi_{2^h}, \ell) = B(\chi_{2^{h-1}}, \ell) + \sum_{j=2}^{2^{h-1}} \sum_{k=0}^{r-1} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} (\zeta_{2^k}^{2h-1+j} + \zeta_{2^k}^{-2h-1-j}) = 2^{r-1} \). This finishes the proof of (4.4).

Suppose that \( 1 < h \leq r - 3, 2^h \nmid \ell \) and \( 2^{r-1} \nmid \ell \). In this case the induction hypothesis implies \( B(\chi_{2^h}, \ell) = 0 \).

Arguing as in the previous paragraph we get

\begin{align*}
B(\chi_{2^h}, \ell) &= \sum_{j=2}^{2h-1} \sum_{k=0}^{r-1} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h-1+j} + \zeta_{2^k}^{-2h-1-j} \right) \zeta_{2^k}^{-\ell}.
\end{align*}

However, if \( j \) is even and smaller than \( 2^{h-1} \) then

\begin{align*}
\sum_{k=0}^{2^{h-1}} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h-1+j} + \zeta_{2^k}^{-2h-1-j} \right) \zeta_{2^k}^{-\ell} = 0.
\end{align*}

Therefore, having in mind that \( \zeta_{2^{h+2}}^2 + \zeta_{2^{h+2}}^{-2h} = 0 \) we have

\begin{align*}
B(\chi_{2^h}, \ell) = \sum_{k=0}^{h} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h} + \zeta_{2^k}^{-2h} \right) \zeta_{2^k}^{-\ell} + 2^{h+1} + \sum_{k=h+3}^{r-1} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h} + \zeta_{2^k}^{-2h} \right) \zeta_{2^k}^{-\ell},
\end{align*}

where \( \epsilon = 1 \) if \( 2^{h+1} \nmid \ell \) and \( \epsilon = -1 \) otherwise. Then the claim follows using the following equalities that can be proved by straightforward calculations:

\begin{align*}
\sum_{k=0}^{h} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h} + \zeta_{2^k}^{-2h} \right) \zeta_{2^k}^{-\ell} &= 2^{h+1} \quad \text{and} \\
\sum_{k=h+3}^{r-1} \Tr_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left( \zeta_{2^k}^{2h} + \zeta_{2^k}^{-2h} \right) \zeta_{2^k}^{-\ell} &= \begin{cases} 
0, & \text{if } 2^{h+1} \nmid \ell; \\
2^{r-1} - 2^{h+2}, & \text{if } 2^{h+1} \nmid \ell \text{ and } \ell \equiv \pm 2^h \text{ mod } 2^{r-1}; \\
-2^{h+2}, & \text{if } 2^{h+1} \nmid \ell \text{ and } \ell \not\equiv \pm 2^h \text{ mod } 2^{r-1}.
\end{cases}
\end{align*}

This finishes the proof of (4.5).
We now prove, by induction on $h$, that the following two statements hold for any integer $0 \leq h \leq r - 3$:

\[(4.6) \quad \sum_{k \in X_h} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}) = \pm 1, \quad \text{where } X_h = \{i \in \{1, \ldots, 2^{r-2}\} : i \equiv \pm 1 \mod 2^{r-h}\};\]

\[(4.7) \quad \varepsilon_i \equiv \varepsilon_j \mod 2^{r-h-1} \text{ if } i \equiv \pm j \mod 2^{r-h-1} \text{ and } i \not\equiv 0, \pm 1 \mod 2^{r-h-1} \text{ then } \varepsilon_i = \varepsilon_j;\]

and that the next one holds for every $0 \leq h \leq r - 2$:

\[(4.8) \quad \text{if } i \equiv 0 \mod 2^{r-h-1} \text{ then } \varepsilon_i = 0.\]

Observe that $X_0 = \{1\}$. Fix an integer $i$. Then for every integer $k$ we have

\[
\text{Tr}_{Q(\zeta_{2^r})/Q} \left( \left( \zeta_{2^r}^k + \zeta_{2^r}^{-k} \right) \zeta_{2^r}^{-i} \right) = \begin{cases} 
2^{r-1}, & \text{if } k \equiv i \mod 2^r; \\
-2^{r-1}, & \text{if } k \equiv 2^{r-1} - i \mod 2^r; \\
0, & \text{otherwise.}
\end{cases}
\]

Thus $A(\chi_1, i) = 2^{r-1} (\varepsilon_i - \varepsilon_{i + 2^{r-1}})$ and hence for $h = 0$, (4.6) and (4.7) follows at once from (4.2), (4.3) and (4.5). Moreover, for $h = 0$ (4.8) is clear because $\varepsilon_{2^{r-1}} = 0$.

Suppose $0 < h \leq r - 3$ and (4.6), (4.7) and (4.8) hold for $h$ replaced by $h - 1$. Suppose also that $i \not\equiv 0 \mod 2^{r-h-1}$. To prove (4.6) and (4.7) we first compute $A(\chi_{2^h}, 2^h i)$ which we split in three summands:

\[
A(\chi_{2^h}, 2^h i) = \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \zeta_{2^r}^{-2^h i} \right) + \sum_{j=2}^{2^{h-2}-2^{r-h-1}-1} \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \left( \zeta_{2^r}^k + \zeta_{2^r}^{-k} \right) \zeta_{2^r}^{-2^h i} \right)
\]

\[+ \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \zeta_{2^r}^{2^h (k-i)} + \zeta_{2^r}^{-2^h (k+i)} \right).
\]

We now prove that the first two summands are 0. This is clear for the first one because $2^{r-1} \nmid 2^h i$. To prove that the second summand is 0 let $2 \leq j \leq 2^h - 2$ and $2 \mid j$. Observe that $2^h \mid j$. Thus, if $k$ is odd then the order of $\zeta_{2^r}^{kj - 2^h i}$ is multiple of $2^{r-h-1}$ and, as $h \leq r - 3$, we deduce that $\text{Tr}_{Q(\zeta_{2^r})/Q} \left( \zeta_{2^r}^{kj - 2^h i} \right) = \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \zeta_{2^r}^{-kj + 2^h i} \right) = 0$. Thus we only have to consider the summands with $k$ even. Actually we can exclude also the summands with $2^{r-h} \mid k$ because, by the induction hypothesis on (4.8), for such $k$ we have $\varepsilon_k = 0$. For the remaining values of $k$ (i.e. $k$ even and not multiple of $2^{r-h}$) we have $\varepsilon_k = \varepsilon_i$ if $k \equiv l \mod 2^{r-h-1}$, by the induction hypothesis on (4.7). So, we can rewrite $\sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \left( \zeta_{2^r}^k + \zeta_{2^r}^{-k} \right) \zeta_{2^r}^{-2^h i} \right)$ as

\[
\sum_{l \in \mathbb{Z}_{2^{r-h-1}}} \varepsilon_l \text{Tr}_{Q(\zeta_{2^r})/Q} \left( \left( \zeta_{2^r}^{-2^h i} \sum_{a=0}^{2^{h-1}} (\zeta_{2^r}^{-2^h i}) a \right) + \zeta_{2^r}^{-2^h i} \left( \sum_{a=0}^{2^{h-1}} (\zeta_{2^r}^{-2^h i}) a \right) \right),
\]

which is 0 because $\zeta_{2^r}^{-2^h i}$ is a root of unity different from 1 and of order dividing $2^h$, as $j$ is even but not multiple of $2^h$. This finishes the proof that the first two summands are 0. To finish the calculation of $A(\chi_{2^h}, 2^h i)$ we compute

\[
\text{Tr}_{Q(\zeta_{2^r})/Q} \left( \zeta_{2^r}^{2^h (k-i)} + \zeta_{2^r}^{-2^h (k+i)} \right) = \begin{cases} 
2^{r-1}, & \text{if } k \in X_{h,i}; \\
-2^{r-1}, & \text{if } k - 2^{r-h-1} \in X_{h,i}; \\
0, & \text{otherwise,}
\end{cases}
\]

where $X_{h,i} = \{k \in \{1, \ldots, 2^{r-2}\} : k \equiv \pm i \mod 2^{r-h}\}$. So we have proved the following:

\[
A(\chi_{2^h}, 2^h i) = 2^{r-1} \sum_{k \in X_{h,i}} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}).
\]
Then (4.6) follows from (4.3), (4.5) and the previous formula. Using (4.2) we also obtain that \( \sum_{k \in X_{h,i}} \varepsilon_k = \sum_{k \in X_{h,i}} \varepsilon_{k+2^{r-h}-1} \) if \( i \not\equiv \pm 1 \mod 2^{r-h-1} \). However, in this case the induction hypothesis for (4.7) means that the \( \varepsilon_k \) with \( k \in X_{h,i} \) are all equal and the \( \varepsilon_{k+2^{r-h}-1} \) with \( k \in X_{h,i} \) are all equal. Hence (4.7) follows.

In order to deal with (4.8), assume that \( 0 < h \leq r - 2 \). By induction hypothesis on (4.8) we have \( \varepsilon_k = 0 \) if \( 2^{r-h} \mid k \), and by the induction hypothesis on (4.7), we have that \( \varepsilon_k \) is constant on the set \( X \) formed by integers \( 1 \leq k \leq 2^{r-1} \) such that \( k \equiv 2^{r-h-1} \mod 2^{r-h} \). We will use these two facts without specific mention. Arguing as before we have

\[
A(\chi_{2^h},0) = \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^h})/Q} \left( 1 + \zeta_{2^h}^h \zeta_{2^h}^{-h} \right) + \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \text{Tr}_{Q(\zeta_{2^h})/Q} \left( \sum_{j=1}^{2^{h-1}-1} (\zeta_{2^h}^{2j} + \zeta_{2^h}^{-2j}) \right)
\]

\[
= \sum_{k=1,2^{r-h} \mid k} \varepsilon_k \text{Tr}_{Q(\zeta_{2^h})/Q} \left( 1 + \zeta_{2^h}^h \zeta_{2^h}^{-h} \right).
\]

As

\[
\text{Tr}_{Q(\zeta_{2^h})/Q} \left( 1 + \zeta_{2^h}^h \zeta_{2^h}^{-h} \right) = \begin{cases} 2^{r-1}, & \text{if } 2^{r-h-1} \mid k; \\ -2^{r-1}, & \text{if } 2^{r-h-1} \nmid k \text{ and } 2^{r-h} \mid k; \end{cases}
\]

we obtain

\[
A(\chi_{2^h},0) = 2^{r-1} \left( \sum_{2^{r-h-1} \mid k} \varepsilon_k - \sum_{2^{r-h-1} \nmid k} \varepsilon_k \right) = 2^{r-1} \left( 1 - 2 \sum_{k \in X} \varepsilon_k \right) = 2^{r-1} (1 - 2 |X| \varepsilon_k).
\]

From (4.3) and (4.4) we deduce that if \( k \in X \) then \( 1 - 2 \varepsilon_k = \pm 1 \) and hence \( \varepsilon_k = 0 \), since \( |X| = 2^{r-h-1} \geq 2 \), as \( h \leq r - 2 \). This finishes the proof of (4.8).

To finish the proof of the proposition it is enough to show that \( \varepsilon_i \neq 0 \) for exactly one \( i \in \{1, \ldots, 2^{r-1} - 1\} \). If \( i \) is even then \( \varepsilon_i = 0 \), by (4.8) with \( h = r - 2 \).

We claim that if \( \varepsilon_i \neq 0 \) then \( i \equiv \pm 1 \mod 2^{r-1} \). Otherwise, there are integers \( 2 \leq v \leq r - 2 \) and \( 2 < i < 2^{r-1} - 1 \) satisfying \( i \not\equiv \pm 1 \mod 2^{v+1} \) and \( \varepsilon_i \neq 0 \). We choose \( v \) minimum with this property for some \( i \). Then (1) \( \varepsilon_k = 0 \) for every \( k \not\equiv \pm 1 \mod 2^v \) and (2) \( i \equiv \pm (k + 2^v) \mod 2^{v+1} \) for every \( k \in X_{r-v-1} \). (1) implies that \( \sum_{k \in X_{r-v-1}} (\varepsilon_k + \varepsilon_{k+2^v}) = 1 \). On the other hand \( 1 \leq r - v - 1 \leq r - 3 \) and hence applying (4.6) and (4.7) with \( h = r - v - 1 \) we deduce from (2) that \( \varepsilon_i = \varepsilon_{k+2^v} \) for every \( k \in X_{r-v-1} \) and \( \sum_{k \in X_{r-v-1}} (\varepsilon_k - \varepsilon_{k+2^v}) = \pm 1 \). Using \( |X_{r-v-1}| = 2^{r-v-1} \) and \( \varepsilon_i \neq 0 \) we deduce that \( 2^{r-v} \varepsilon_i = 2 \sum_{k \in X_{r-v-1}} \varepsilon_k + 2^{r-v} = 2 \), in contradiction with \( 2 \leq r - v \). This finishes the proof of the claim.

Then the only possible non-zero partial augmentations of \( u \) are \( \varepsilon_1 \) and \( \varepsilon_{2^{r-1}-1} \). Hence \( \varepsilon_1 + \varepsilon_{2^{r-1}-1} = 1 \) and, by applying (4.6) with \( h = 0 \) we deduce that \( \varepsilon_1 - \varepsilon_{2^{r-1}-1} = \pm 1 \). Therefore, either \( \varepsilon_1 = 0 \) or \( \varepsilon_{2^{r-1}-1} = 0 \), i.e. \( \varepsilon_i \neq 0 \) for exactly one \( i \in \{1, \ldots, 2^{r-1} - 1\} \), as desired.

5. Proof of Theorem 1.1

In this section we prove Theorem 1.1. Recall that \( G = \text{SL}(2,q) \) with \( q = t^f \) and \( t \) an odd prime number, \( G = \text{PSL}(2,q) \), \( \pi : G \rightarrow G \) is the natural projection and \( u \) is an element of order \( n \) in \( V(ZG) \) with \( \gcd(n,q) = 1 \). We have to show that \( u \) is rationally conjugate to an element of \( G \). By Proposition 3.1.(4), we may assume that \( n \) is multiple of 4 and by Proposition 4.1 that \( n \) is not a prime power. Moreover, we may also assume that \( n \neq 12 \) because this case follows easily from known results and the HeLP Method. Indeed, if \( n = 12 \) then \( \pi(u) \) has order 6, by Proposition 3.1.(2) and hence \( \pi(u) \) is rationally conjugate to an element of \( G \), by [Her07, Proposition 6.6]. Using this and the fact that \( G \) has a unique conjugacy class for each of the orders 3, 4 or 6 and two conjugacy classes of elements of order 12, and applying (D) with \( \chi = \chi_1 \) and \( \ell = 1,5 \) it easily follows that all the partial augmentations of \( u \) are non-negative. This can be also obtained using the GAP Package [BM17a],
In the remainder we follow the strategy of the proof of the main result of [MRS18]. The difference with the arguments of that paper is twofold: On the one hand, in our case \( n \) is even (actually multiple of 4) and this introduces some difficulties not appearing in [MRS18] where \( n \) was odd. On the other hand for \( \text{SL}(2, q) \) we have more Brauer characters than for \( \text{PSL}(2, q) \) and this will help to reduce some cases.

As the order \( n \) of \( u \) is fixed throughout, we simplify the notation of the Section 2 by setting

\[
\gamma = \gamma_n, \quad \bar{\gamma} = \bar{\gamma}_n, \quad \alpha_x = \alpha_x^{(n)}(n), \quad \kappa_x = \kappa_x^{(n)}, \quad \beta_{h,x} = \beta_{h,x}^{(n)}, \quad \mathcal{B} = \mathcal{B}_n, \quad \mathcal{B} = \mathcal{B}_n.
\]

We argue by induction on \( n \). So we also assume that \( u^d \) is rationally conjugate to an element of \( G \) for every divisor \( d \) of \( n \) with \( d \neq 1 \).

We will use the representations \( \Theta_m \) and \( t \)-Brauer characters \( \chi_m \) introduced in (3.1). Observe that the kernel of \( \Theta_m \) is trivial if \( m \) is odd, and otherwise it is the center of \( G \). Using this and the induction hypothesis on \( n \) it easily follows that the order of \( \Theta_m(u) \) is \( \frac{n}{2} \) if \( m \) is even, while, if \( m \) is odd then the order of \( \Theta_m(u) \) is \( n \). Combining this with Proposition 3.1.(7) we deduce that \( \Theta_1(u) \) is conjugate to \( \text{diag}(\zeta, \zeta^{-1}) \) for a suitable primitive \( n \)-th root of unity \( \zeta \). Hence there exists an element \( g_0 \in G \) of order \( n \) such that \( \Theta_1(g_0) \) and \( \Theta_1(u) \) are conjugate. The element \( g_0 \in G \) and the primitive \( n \)-th root of unity \( \zeta \) will be fixed throughout and from now on we abuse the notation and consider \( \zeta \) both as a primitive \( n \)-th root of unity in a field of characteristic \( t \) and as a complex primitive \( n \)-th root of unity. Then

\[
\Theta_m(g_0) \text{ is conjugate to } \begin{cases} 
\text{diag} \left( 1, \zeta^2, \zeta^{-2}, \ldots, \zeta^m, \zeta^{-m} \right), & \text{if } 2 \mid m; \\
\text{diag} \left( \zeta, \zeta^{-1}, \zeta^3, \zeta^{-3}, \ldots, \zeta^m, \zeta^{-m} \right), & \text{if } 2 \nmid m;
\end{cases}
\]

and

\[
\chi_m(g_0^j) = \sum_{j=-m \text{ mod } 2}^m \zeta^{ij} = \begin{cases} 
1 + \alpha_{2i} + \alpha_{4i} + \cdots + \alpha_{mi}, & \text{if } 2 \mid m; \\
\alpha_i + \alpha_{3i} + \cdots + \alpha_{mi}, & \text{if } 2 \nmid m.
\end{cases}
\]  

By the induction hypothesis on \( n \), if \( c \) is a divisor of \( n \) with \( c \neq 1 \) then \( u^c \) is rationally conjugate to \( g_0^i \) for some \( i \) and hence \( \zeta^c = \zeta^{\pm i} \). Therefore \( c \sim_n i \) and hence \( u^c \) is conjugate to \( g_0^c \).

By (E), two elements of \( \langle g_0 \rangle \) are conjugate in \( G \) if and only if they are equal or mutually inverse. Moreover, every element \( g \in G \), with \( g^n = 1 \), is conjugate to an element of \( \langle g_0 \rangle \). Therefore \( x \mapsto (g_0^x)^G \) induces a bijection from \( \Gamma_n \) to the set of conjugacy classes of \( G \) formed by elements of order dividing \( n \). For an integer \( x \) (or \( x \in \Gamma_n \)) we set

\[
\varepsilon_x = \varepsilon_{g_0^x}(u) \quad \text{and} \quad \lambda_x = \sum_{i \in \Gamma_n} \varepsilon_i \alpha_{ix}.
\]

Our main tool is the following lemma whose proof is exactly the same as the one of Lemma 4.1 in [MRS18]. We also collect Corollary 3.3 of this paper.

**Lemma 5.1.** \( u \) is rationally conjugate to \( g_0 \) if and only if \( \lambda_i = \alpha_i \), for any positive integer \( i \).

For a positive integer \( n \) and a subfield \( F \) of \( \mathbb{Q}(\zeta_n) \), let \( \Gamma_F \) denote a set of representatives of equivalence classes of the following equivalence relation defined on \( \mathbb{Z} \):

\[
x \sim y \quad \text{if and only if} \quad \zeta_n^x \text{ and } \zeta_n^y \text{ are conjugate in } \mathbb{Q}(\zeta_n) \text{ over } F.
\]

**Corollary 5.2.** Let \( n \) be a positive integer, let \( F \) be a subfield of \( \mathbb{Q}(\zeta_n) \) and let \( R \) be the ring of integers of \( F \). For every \( x \in \Gamma_F \) let \( B_x \) be an integer and for every integer \( i \) define

\[
\omega_i = \sum_{x \in \Gamma_F} B_x T_{\mathbb{Q}(\zeta_n)/F}(\zeta_n^{ix}).
\]

Let \( d \) be a divisor of \( n \) such that \( \omega_q = 0 \) for every prime power \( q \) dividing \( d \) with \( q \neq 1 \). Then \( \omega_d \in d \cdot R \).
By Lemma 5.1, in order to achieve our goal it is enough to prove that \( \lambda_i = \alpha_i \) for every positive integer \( i \). We argue by contradiction, so we assume that \( \lambda_d \neq \alpha_d \) for some positive integer \( d \) which we assume to be minimal with this property. Observe that if \( \lambda_i = \alpha_i \) and \( j \) is an integer such that \( \gcd(i, n) = \gcd(j, n) \), then there exists \( \sigma \in \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \) such that \( \sigma(\alpha_i) = \alpha_j \) and applying \( \sigma \) to the equation \( \lambda_i = \alpha_i \) we obtain \( \lambda_j = \alpha_j \). This implies that \( d \) divides \( n \). Note that \( \alpha_1 = \lambda_1 \), by our choice of \( g_0 \), and hence \( d \neq 1 \). Moreover, \( d \neq n \) because \( \lambda_n = 2 \sum_{x \in \Gamma_n} \varepsilon_x = 2 = \alpha_n \) as the augmentation of \( u \) is 1.

We claim that

\[
\lambda_d = \alpha_d + d \tau \quad \text{for some } \tau \in \mathbb{Z}[\alpha_1].
\]

Indeed, for any \( x \in \Gamma_n \) let \( B_x = \varepsilon_x - 1 \) if \( x \sim n \) and \( B_x = \varepsilon_x \) otherwise. Then for any integer \( i \) we have

\[
\lambda_i - \alpha_i = \sum_{x \in \Gamma_n} B_x \text{Tr}_{\mathbb{Q}(\xi)/\mathbb{Q}(\alpha)}(\xi^i x).
\]

The claim then follows by applying Corollary 5.2 with \( F = \mathbb{Q}(\alpha_1) \), \( R = \mathbb{Z}[\alpha_1] \) and \( \omega_i = \lambda_i - \alpha_i \). Observe that in the notation of that corollary \( \Gamma_n = \Gamma_F \).

By (5.1) we have

\[
\chi_d(g_0) = \sum_{i \equiv d \mod 2} \alpha_i \quad \text{and} \quad \chi_d(u) = \sum_{x \in \Gamma_n} \varepsilon_x \chi_d(g_0^x) = \sum_{x \in \Gamma_n} \varepsilon_x \sum_{i \equiv d \mod 2} \alpha_i \nu_x = \sum_{i \equiv d \mod 2} \lambda_i.
\]

Combining this with (5.2) and the minimality of \( d \), we deduce that \( \chi_d(u) = \chi_d(g_0) + d \tau \). Furthermore, \( \tau \neq 0 \), as \( \lambda_d \neq \alpha_d \). Therefore

\[
C_b(\chi_d(u)) \equiv C_b(\chi_d(g_0)) \mod d \quad \text{for every } b \in \mathbb{B}
\]

and

\[
d \leq |C_{b_0}(\chi_d(u)) - C_{b_0}(\chi_d(g_0))| \quad \text{for some } b_0 \in \mathbb{B}.
\]

The bulk of our argument relies on an analysis of the eigenvalues of \( \Theta_d(u) \) and the induction hypothesis on \( n \) and \( d \). More precisely, we will use (5.4) and (5.5) to obtain a contradiction by comparing the eigenvalues of \( \Theta_d(g_0) \) and \( \Theta_d(u) \). Of course, we do not know the eigenvalues of the latter. However we know the eigenvalues of \( \Theta_d(u^c) \) for every \( c \mid n \) with \( c \neq 1 \), because we know the eigenvalues of \( \Theta_d(g_0) \) and \( u^c \) is conjugate to \( g_0^c \).

This provides information on the eigenvalues of \( \Theta_d(u) \). For example, recall that if \( \xi \) is an eigenvalue of \( \Theta_d(u) \) then \( \xi \) and \( \xi^{-1} \) have the same multiplicity as eigenvalues of \( \Theta_d(u) \). Therefore, if \( 3 \leq h \) then the sum of the multiplicities of the eigenvalues of \( \Theta_d(u) \) of order \( h \) is even. Moreover, for every \( t \)-regular element \( g \) of \( G \), the multiplicity of 1 as eigenvalue of \( \Theta_d(g) \) is congruent modulo 2 with the degree \( d + 1 \) of \( \chi_d \). As \( n \) is not a prime power there is an odd prime \( p \) dividing \( n \). By the induction hypothesis \( \Theta_d(u^p) \) is rationally conjugate to \( \Theta_d(g_0^p) \).

Thus the multiplicity of -1 as eigenvalue of \( \Theta_d(u^p) \) is even. As the latter is the sum of the multiplicities as eigenvalues of \( \Theta_d(u) \) of -1 and the elements of order \( 2p \), we deduce that the multiplicity of -1 as eigenvalue of \( \Theta_d(u) \) is even. Using this we can see that \( \Theta_d(u) \) is conjugate to \( \text{diag}(\zeta^\nu, \zeta^{\nu+1}, \ldots, \zeta^{\nu+\delta}) \) for integers \( \nu, \ldots, \nu+\delta \) such that \( \nu-i = -\nu_i \) for every \( i \).

Let \( X_d = \{ i : 1 \leq i \leq d, i \equiv d \mod 2 \} \). Then, by (5.3) and Proposition 2.2, we have for every \( b \in \mathbb{B} \)

\[
C_b(\chi_d(u)) - C_b(\chi_d(g_0)) = \sum_{i \in X_d} \left( \kappa_{n/i} \cdot \beta_{b,i} \cdot \mu(\gamma(i)) \cdot \delta_{b,i}^{(n/i)}(\nu_i) - \kappa_i \cdot \beta_{b,i} \cdot \mu(\gamma(i)) \cdot \delta_{b,i}^{(n/i)}(i) \right).
\]

Moreover, if \( c \mid n \) with \( c \neq 1 \) then the lists \((\nu_i)_{i \in X_d} \) and \((c\bar{c})_{i \in X_d} \) represent the same elements in \( \Gamma_n \), up to ordering, and hence \((\nu_i)_{i \in X_d} \) and \((i)_{i \in X_d} \) represent the same elements of \( \Gamma_{\frac{n}{2}} \), up to ordering. We express this by writing \((\nu(X_d)) \sim_{\frac{n}{2}} (X_d) \). This provides restrictions on \( d \), \( n \) and the \( \nu_i \).

The following two lemmas are variants of Lemmas 4.2 and 4.3 of [MRS18].
Lemma 5.3.  (1) Let $i \in X_d$. If $\kappa_i \ne 1$ then $n = 2d$ and $i = d$. If $\kappa_i \ne 1$ then $\frac{n}{d}$ is the smallest prime dividing $n$ and $\kappa_{\nu_j} = 1$ for every $j \in X_d \setminus \{i\}$.

(2) If $d > 2$ then $n$ is not divisible by any prime greater than $d$. In particular, if $d$ is prime then $\kappa_{\nu_j} = 1$ for every $i \in X_d$.

Proof. Let $p$ denote the smallest prime dividing $n$.

(1) The first statement is clear. Suppose that $\kappa_{\nu_j} \ne 1$. Then either $p = 2$ and $\nu_j \equiv 0 \pmod{\frac{n}{2}}$ or $\nu_j \equiv 0 \pmod{n}$. As $(X_d) \sim \frac{n}{p} (\nu(X_d))$ we deduce that $k \equiv 0 \pmod{\frac{n}{p}}$ for some $k \in X_d$. Therefore $d = k = \frac{n}{p}$ and for every $j \in X_d \setminus \{i\}$ we have $\nu_j \equiv 0 \pmod{\frac{n}{p}}$. Thus $\kappa_{\nu_j} = 1$.

(2) Suppose that $q$ is a prime divisor of $n$ with $d < q$. Then $\frac{n}{d} \ne p$ and therefore, by (1), $\kappa_i = \kappa_{\nu_j} = 1$ for every $i \in X_d$. Thus, by (5.5) and (5.6), it is enough to show that $\delta_{\nu_j}^{(n/\gamma)}(i) \ne 0$ for at most one $i \in X_d$ and $\delta_{\nu_j}^{(n/\gamma)}(i) \ne 0$ for at most one $i \in X_d$. Observe that if $i \in X_d$ then $q \mid i$ and hence $\frac{n}{\gamma(i)}$ is multiple of $q$. Moreover, if $i$ and $j$ are different elements of $X_d$ then $i$ and $j$ have the same parity and $-q < i - j < i + j < 2q$. Therefore $i \not\sim_q j$. Thus either $\delta_{\nu_j}^{(n/\gamma)}(i) = 0$ or $\delta_{\nu_j}^{(n/\gamma)}(i) = 0$. As $(X_d) \sim_q (\nu(X_d))$, this also proves that $\delta_{\nu_j}^{(n/\gamma)}(i) = 0$ or $\delta_{\nu_j}^{(n/\gamma)}(i) = 0$. □

We obtain an upper bound for $|C_b(\chi_d(u)) - C_b(\chi_d(g_0))|$ in terms of the number of prime divisors $P(d)$ of $d$.

Lemma 5.4. For every $b \in \mathbb{B}$ we have $|C_b(\chi_d(u)) - C_b(\chi_d(g_0))| \le 2 + 2P(d)+1$.

Proof. Using (5.6) it is enough to prove that $\sum_{\nu \in X_d} \kappa_i \delta_{\nu_j}^{(n/\gamma)}(i) \le 1 + 2P(d)$ and $\sum_{i \in X_d} \kappa_i \delta_{\nu_j}^{(n/\gamma)}(i) \le 1 + 2P(d)$.

This is a consequence of Lemma 5.3.(1) and the following inequalities for every $e$ dividing $d'$:

$$\left| \left\{ i \in X_d : \gcd(d,e) = 1, \delta_{\nu_j}^{(n/\gamma)}(i) = 1 \right\} \right| \le 1, \quad \left| \left\{ i \in X_d : \gcd(d,e) = 0, \delta_{\nu_j}^{(n/\gamma)}(i) = 1 \right\} \right| \le 1.$$

We prove the second inequality, only using that $(\nu(X_d)) \sim_d (X_d)$. This implies the first inequality by applying the second one to $u = g_0$.

Let $Y_e = \left\{ i \in X_d : \gcd(d,e) = 1, \delta_{\nu_j}^{(n/\gamma)}(i) = 1 \right\}$. By changing the sign of some $\nu_j$'s, we may assume without loss of generality that if $\delta_{\nu_j}^{(n/\gamma)}(i) = 1$ then $b \equiv \nu_j \pmod{\frac{n}{\gamma(i)}}$. Thus, if $i \in Y_e$ then $b \equiv \nu_j \pmod{\frac{n}{\gamma(i)}}$. We claim that if $i, j \in Y_e$ then $\nu_i \equiv \nu_j \pmod{d}$. Indeed, let $p$ be prime divisor of $d$. If $n_p \ne d_p$ or $p \mid e$ then clearly $\nu_i \equiv \nu_j \pmod{d_p}$. Otherwise, i.e. $n_p = d_p$ and $p \mid e$, then $p$ divides both $\gamma(i)$ and $\gamma(j)$ and $\nu_i \equiv \nu_j \pmod{d_p}$. Therefore, by Lemma 2.1.(2), $\nu_i \equiv \nu_j \pmod{d_p}$, as desired. As $(\nu(X_d)) \sim_d (X_d)$ and the elements of $X_d$ represent different classes in $\Gamma_d$ we deduce that $|Y_e| \le 1$. This finishes the proof of the lemma. □

We are ready to finish the proof of Theorem 1.1. Recall that we are arguing by contradiction.

By (5.5) and Lemma 5.4 we have $d \le 2 + 2P(d)+1$ and, using this, it is easy to show that $d \le 6$ or $d = 10$. Indeed, if $P(d) \ge 3$ then $2 + 2P(d)+1 \ge d \ge 2 \cdot 3 \cdot 5 \cdot 2P(d)-3 > 14 + 2P(d)+1$, a contradiction. Thus $P(d) = 2$ and $d \le 10$ or $P(d) = 1$ and $d \le 5$. Hence $d$ is either 2, 3, 4, 5, 6 or 10. We deal with these cases separately.

Suppose that $d = 2$. Then $\nu_2 \sim_{\nu_2} 2$ for every prime $p$. By the assumptions on $n$ and Lemma 5.3.(1), this implies that $\kappa_2 = \kappa_{\nu_2} = 1$, $\gamma(2) = \nu(2)$ and $\beta_{\nu_1,2} = \beta_{\nu_1,\nu_2}$. Therefore $|C_{b_0}(\chi_2(u)) - C_{b_0}(\chi_2(g_0))| = \mu(\gamma(2)) \left( \delta_{\nu_1,\nu_2}^{(n/\gamma)(2)} - \delta_{\nu_1,\nu_2}^{(n/\gamma)(2)} \right) \le 1$, contradicting (5.5).

Suppose that $d = 3$. By Lemma 5.3 and the assumptions on $n$, we have $\kappa_i = \kappa_{\nu_j} = 1$ for every $i \in X_3$ and $\nu_i = 6$. If $2^4 \mid n$ or $3^2 \mid n$ then $\left\{ i = 1, 3 : \delta_{\nu_1,3}^{(n/\gamma)}(i) = 1 \right\} \le 1$ and $\left\{ i = 1, 3 : \delta_{\nu_1,\nu_j}^{(n/\gamma)}(i) = 1 \right\} \le 1$, which implies $|C_{b_0}(\chi_3(u)) - C_{b_0}(\chi_3(g_0))| \le 2$, contradicting (5.5). Thus $n = 24$, since $n$ is neither 12 nor a prime power and it is multiple of 4. In this case we have $\gamma(1) = \gamma(2) = 2, \gamma(3) = \gamma(2) = 3, \beta_{\nu_1,3} = \beta_{\nu_1,\nu_3} = 1$ and $C_{b_0}(\chi_3(g_0)) = -\delta_{\nu_1}^{(12)} - \delta_{\nu_3}^{(8)}$ for every $b \in \mathbb{B}$. We may assume that $3 \mid \nu_3$ and $3 \nmid \nu_1$ because $(\nu(X_3)) \sim_3 (X_3)$. Suppose that $\nu_3 \sim_3 3$ and $\nu_1 \sim_3 1$. Then $\gamma(\nu_1) = \nu(\nu_1) = 2, \gamma(\nu_3) = \gamma(\nu_3) = 3, \beta_{\nu_0,\nu_3} = 1 = \delta_{\nu_0,\nu_3} = 0$, which implies $|C_{b_0}(\chi_3(u)) - C_{b_0}(\chi_3(g_0))| \le 2$, contradicting (5.5). Suppose now that $\nu_3 \sim_3 1$ and $\nu_1 \sim_3 3$. This implies that $\nu_1 \equiv \pm 3 \pmod{8}$ and $\nu_1 \equiv \pm 1 \pmod{3}$ (because $3 \mid \nu_3$ but $3 \nmid \nu_1$). Thus either $\nu_1 \equiv \pm 11 \pmod{24}$ or

\[11\]
ν₁ ≡ ±5 mod 24. As (ν(X₃)) ~₁₂ (X₃), we deduce that the only possibility is ν₁ ≡ ±11 mod 24. In this case we have γ(ν₁) = γ(ν₁) = 1 and γ(ν₃) = γ(ν₃) = 6. Hence C₁₁(χ₃(u)) = C₁₁(χ₃(g₀)) = δ₁₂(4) + δ₁₂(12) + δ₁₂(8) = 4, contradicting (5.4).

Suppose that d = 4. By Lemma 5.3 and the assumptions on n, we have κᵢ = κᵢ = 1 for every i ∈ X₄ and n' = 6. If 3³ | n or 2³ | n then \( \left| \left\{ i = 2, 4 : \delta_{b,i}^{(n/3)(i)} = 1 \right\} \right| \leq 1 \) which implies |C₀(χₙ(u)) − C₀(χₙ(g₀))| ≤ 3, contradicting (5.5). Thus n = 36. In this case we have γ(2) = 1 = β₀,2 = β₀,4 and γ(4) = 2, which implies |C₀(χₙ(g₀))| ≤ 1 and hence |C₀(χₙ(u)) − C₀(χₙ(g₀))| ≤ 3, contradicting again (5.5).

Suppose that d = 5. Since (ν(X₅)) ~₁₂ (X₅), there is exactly one νᵢ which is divisible by 5, say ν₅. In particular, for i ≠ 5 we have 5 ∣ \( n/n(ν_i) \) and 5 ∣ \( n/n(ν_i) \). Moreover, if j is an integer not multiple of 5 then \( \left| \left\{ i = 1, 3 : ν_i \sim_j \right\} \right| \leq 1 \). This implies that \( \left| \left\{ i = 1, 3 : \delta_{b,i}^{(n/5)(i)} = 1 \right\} \right| \leq 1 \) and \( \left| \left\{ i = 1, 3 : \delta_{b,i}^{(n/5)(ν_i)} = 1 \right\} \right| \leq 1 \). On the other hand, as n ≠ 10, we deduce that κᵢ = 1 for every i ∈ X₅, by Lemma 5.3.(1). Therefore, using (5.5) and (5.6), we deduce that κᵢ = 2, in contradiction with Lemma 5.3.(1).

Suppose that d = 6. By Lemma 5.3, we have n’ | 30 and κᵢ = κᵢ = 1 for every i ∈ X₆ because n ≠ 12. If 25 | n, or 9 | n or 8 | n then we have \( \left| \left\{ i = 2, 4, 6 : \delta_{b,i}^{(n/5)(i)} = 1 \right\} \right| \leq 2 \) and \( \left| \left\{ i = 2, 4, 6 : \delta_{b,i}^{(n/5)(ν_i)} = 1 \right\} \right| \leq 2 \). This implies that |C₀(χ₆(u)) − C₀(χ₆(g₀))| ≤ 4, yielding a contradiction with (5.5). Therefore n = 60 and hence β₀,2 = β₀,4 = β₀,6 = 1, γ(2) = 1, γ(4) = 4, and γ(6) = 6. This implies that |C₀(χ₆(ν₆))| ≤ 2 and hence |C₀(χ₆(u)) − C₀(χ₆(g₀))| ≤ 5, yielding a contradiction with (5.5).

Suppose that d = 10. If 5 | \( n/n(ν_i) \) for some i ∈ X₁₀ then n₅ = (γ(νᵢ))₅ = 5 and hence 5 | i. The same also holds for νᵢ. Therefore, if 5 | i then 5 | \( n/n(ν_i) \) and if 5 | νᵢ then 5 | \( n/n(ν_i) \). Thus \( \left| \left\{ i ∈ X₁₀ : 5 | i, \delta_{b,i}^{(n/5)(ν_i)} = 1 \right\} \right| \leq 2 \). This implies that |C₀(χ₁₀(ν₁)) − C₀(χ₁₀(g₀))| ≤ 8, contradicting (5.5).

REFERENCES


Email address: adelrio@um.es

Email address: mariano.serrano@um.es

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MURCIA.